REMARKS

In response to the Office Action mailed July 2, 2004, the Applicant respectfully requests reconsideration. To further the prosecution of this Application, the Applicant submits the following remarks, has canceled claims and has added new claims. The claims as now presented are believed to be in allowable condition.

Claims 1-29 were pending in this Application. By this Amendment, claims 2, 8, 15, and 18 have been canceled and claims 30-35 have been added. Accordingly, claims 1, 3-7, 9-14, 16-17, and 19-35 are now pending in this Application. Claims 1, 7, 13, 14, 17, 20, 21, 23, 25, 26, 28, and 35 are independent claims and the remaining claims are dependent claims.

Rejections under 35 U.S.C. §103

Claims 1-29 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,506,961 to Carlson et al. (hereafter Carlson) in view of U.S. Patent No. 6,279,111 to Jensenworth et al. (hereafter Jensenworth). The Applicant asserts that the present claimed invention is not anticipated by any disclosure in either the Carlson reference or the Jensenworth reference either alone or in combination. Reconsideration of the rejection is respectfully requested.

Claim Amendments

Claims 1, 13, 26, and 28 have been amended to include subject matter found in previously examined claim 2. Claim 7 has been amended to include subject matter found in previously examined claim 8. Claim 14 has been amended to include subject matter found in previously examined claim 15. Claims 17 and 20 have been amended to include subject matter found in previously examined claim 18. No new matter has been added to the application by the aforementioned claim amendments. Accordingly, with respect to claims 1, 7, 13, 14, 17, 20, 26 and 28, the Applicant has not amended these claims in a manner that requires further searching and consderation.

Furthermore, claim 21 has been voluntarily amended to correct a typographical error. Claim 21 now recites, in part, a processor configured to "provide through the input/output controller to the data storage system the request to access the set of data and a first access token that provides access to the set of storage locations". Such recitation is found within previously examined independent claims 23 and 25. No new matter has been added to the application by the claim amendment. Accordingly, with respect to claim 21, the Applicant has not amended these claims in a manner that requires further searching and consderation.

Newly Added Claims

Claims 30-35 have been added and are believed to be in allowable condition. Support for claims 30-32 is provided within the specification on page 4, lines 11-15, for example. Addition of these claims does not add new matter the application. Support for claims 33-35 is provided within the specification on page 4, lines 1-10, for example. Addition of these claims does not add new matter the application.

The Carlson and Jensenworth References

Carlson relates to the authorization of peer-to-peer connections.[1] In Carlson, to obtain information required by a user and/or an application program, a client connection manager issues a request to a system authorizer.[2] Furthermore, in Carlson,

> [s]ince the client application may or may not know the location of the desired information, the request may or may not include the address of a server device (i.e., the client connection manager will not provide the address of a server device when the location of the information is unknown to it). When the system authorizer receives the request, it first verifies that the client device is who it claims to be. The system authorizer then identifies the applicable server device by using either the address provided by the client connection manager or the information contained in the request. If the system authorizer determines that the client device should be allowed to access the information on the subject server device, it then sends

---

1 Carlson, col. 1, l. 11-12.

2 Carlson, col. 3, l. 56-58.

> a token to the server device and a copy of the same token to the client device...
>
> Upon receipt of the token copy from the system authorizer, the client connection manager packages the token copy into a message that it sends to the server device. When the server connection manager receives the message from the client device, it compares the token copy to the token it received from the system authorizer. If the tokens match, the server connection manager responds to the client device and the connection is established. If the tokens do not match, the server connection manager notifies the system authorizer of the failed connection attempt and then proceeds to inform the client device.[3]

Jensenworth relates to a security model for computer systems.[4] Jensenworth provides restricted access tokens, each of which are a modified, restricted version of an access token created from an existing (parent) token.[5] During operation, in Jensenworth,

> a process is associated with a restricted token, such as by an application that launches that process. When the restricted process attempts to perform an action on a resource [e.g., a file object], a kernel mode security mechanism first compares the user-based security identifiers and the intended type of action against a list of identifiers and actions associated with the resource. If there are no restricted security identifiers in the restricted token, access is determined by the result of this first comparison. If there are restricted security identifiers in the restricted token, a second access check for this action compares the restricted security identifiers against the list of identifiers and actions associated with the resource. With a token having restricted security identifiers, the process is granted access to the resource only if both the first and second access checks pass.[6]

Rejections under §103(a)

Independent claims 1, 7, 13, 14, 17, 20, 21, 23, 25, 26, and 28, as amended, are rejected under 35 U.S.C. §103(a) as being unpatentable over Carlson in view of Jensenworth.

In order to establish a *prima facie* case of obviousness, the Office Action must meet three criteria.

---

3 Carlson, col. 3, l. 58 – col. 4, l. 21 (emphasis added).
4 Jensenworth, col. 1, l. 6-7.
5 Jensenworth, col. 1, l. 55-57.
6 Jensenworth, col. 1, 66 – col. 2, l. 13 (emphasis added).

> "First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations."[7]

The Applicant's amended independent claims 1, 7, 13, 14, 17, 20, 26, and 28 generally relate to a data storage system or data storage assembly that includes a set of storage locations that stores a set of data. The data storage system or data storage assembly receives from a host in communication with the data access manager (i) a request to access the set of data and (ii) a first access token of the plurality of tokens that provides access to the set of data stored in the set of storage locations. The data storage system or data storage assembly generates an authorization signal that controls access to the set of data based on the first access token and a second access token of the plurality of tokens, the second access token associated with the set of storage locations, by performing a comparison of the first access token to the second access token associated with the set of storage locations. If the comparison indicates that the first access token and the second access token are identical, the data storage system or data storage assembly produces an access approval signal that provides access to the set of storage locations. If the comparison indicates that the first access token and the second access token are not identical, the data storage system or data storage assembly produces an access failure signal that indicates a denial of access to the set of storage locations.

The Office Action has not established a *prima facie* case of obviousness with respect to the Applicant's independent claims 1, 7, 13, 14, 17, 20, 26, and 28 because neither Carlson nor Jensenworth, taken alone or in combination, teach or suggest all of the claim limitations of claims 1, 7, 13, 14, 17, 20, 26, and 28.

The Office Action states that Carlson does not teach the implementation of "a first token to get and generate an authorization signal that controls access to the set of data based on the first access token and a second access token of the plurality of tokens, the

---

[7] *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

second token associated with the set of storage locations", such as claimed by the Applicant in claims 1, 7, 13, 14, 17, 20, 26, and 28. Furthermore, Carlson does not teach or suggest generation of an authorization signal to provide access or denial of access to a set of storage locations, to access a set of data, based upon a comparison of a first access token and a second access token, as claimed by the Applicant.

As indicated above, in Carlson, when a system authorizer receives a request, it first verifies that the client device is who it claims to be. If the system authorizer determines that the client device should be allowed to access the information on the subject server device, it then sends a token to the server device and a copy of the same token to the client device. Upon receipt of the token copy from the system authorizer, the client connection manager packages the token copy into a message that it sends to the server device. When the server connection manager receives the message from the client device, it compares the token copy to the token it received from the system authorizer. If the tokens match, the server connection manager responds to the client device and the connection is established (e.g., the connection with the server device). If the tokens do not match, the server connection manager notifies the system authorizer of the failed connection attempt and then proceeds to inform the client device.

Carlson, however, does not teach or suggest "generation of an authorization signal to provide access or denial of access to a set of storage locations (e.g., of a data storage assembly), to access a set of data, based upon a comparison of a first access token and a second access token", as claimed by the Applicant. In Carlson, based upon a comparison of the client token and the system authorizer token, the server connection manager determines whether the client device should be allowed to access the information on the subject server device (e.g., a connection is established with the server). The storage device of Carlson is not analogous to the Applicant's storage device locations. The Applicant's storage device locations relate to specific locations within a data storage assembly (e.g., storage device), as opposed to the data storage assembly or storage device itself, as described in Carlson.

Furthermore, Jensenworth does not teach or suggest generation of an authorization signal to provide access or denial of access to a set of storage locations, to

access a set of data, based upon a comparison of a first access token and a second access token, as claimed by the Applicant. As described in Jensenworth, when a restricted process attempts to perform an action on a resource [e.g., a file object], a kernel mode security mechanism first compares user-based security identifiers of a restricted token of the restricted process against a list of identifiers and actions associated with the resource. If there are no restricted security identifiers in the restricted token, access to the resource is determined by the result of the comparison.

While Jensenworth does describe comparing a restricted token against a list of identifiers, Jensenworth does not teach or suggest performing a comparison of the first access token to the second access token, as claimed by the Applicant. Additionally, while Jensenworth does describe providing access to a resource or file object as determined by the result of the comparison of the restricted token against the list of identifiers, Jensenworth does not teach or suggest providing or denying access to a set of storage locations, as claimed by the Applicant.

Because neither Carlson nor Jensenworth, taken alone or in combination, teaches or suggests every element of the Applicants' independent claims 1, 7, 13, 14, 17, 20, 26, and 28, the claims are patentable over Carlson and Jensenworth and should be allowed to issue. Accordingly, the rejection of these claims should be withdrawn. Claims 3-6, 27, 29 which depend on claim 1, claims 9-12, which depend upon claim 7, claim 16, which depend upon claim 14, and claim 19 which depend upon claim 17 should also be allowed to issue as depending upon allowable independent claims (i.e., for at least the reasons presented). Reconsideration of the rejection is respectfully requested.

The Office Action has not established a *prima facie* case of obviousness with respect to the Applicant's independent claims 21, 23, and 25 because neither Carlson nor Jensenworth, taken alone or in combination, teach or suggest all of the claim limitations of claims 21, 23, and 25

Claims 21, 23, and 25 relate to a host device that requests access to a set of data stored in a set of storage locations in a data storage system. The host device generates a request to access the set of data stored in the set of storage locations and provides, through an input/output controller to the data storage system, the request to access the set

of data and a first access token that provides access to the set of storage locations. The host device, further, obtains, through the input/output controller from the data storage system, a response signal that provides a response to the request based on the first access token and a second access token associated with each storage location.

With respect to rejection of independent claim 23, the Office Action incorporates the rejection of claim 1 and states that "Carlson does teach the access privilege of the PWS as to read or write from a particular storage device location (Col. 8, lines 1-5). Upon closer review, however, Carlson in Col. 8, lines 1-5, indicates that "the multimedia application running on PWS 300 may want to be authorized to write as well as read from a particular storage device". As indicated above, the storage device of Carlson is not analogous to the Applicant's storage device locations. The Applicant's storage device locations relate to specific locations within a data storage assembly (e.g., storage device), as opposed to the data storage assembly or storage device itself, as described in Carlson.

As such, Carlson does not teach or disclose a host providing a "request to access the set of data and a first access token that provides access to the set of storage locations", as claimed by the Applicant. Additionally, Jensenworth describes providing access to a resource or file object. Jensenworth does not teach or suggest providing a "request to access the set of data and a first access token that provides access to the set of storage locations", as claimed by the Applicant.

With respect to claims 21 and 25, the Office Action incorporates the rejection of claim 1 and indicates that Carlson teaches an input/output controller to the data storage system. As with the rejection to claim 23, Carlson does not teach or disclose a host providing a "request to access the set of data and a first access token that provides access to the set of storage locations", as claimed by the Applicant. Additionally, Jensenworth does not teach or suggest providing a "request to access the set of data and a first access token that provides access to the set of storage locations", as claimed by the Applicant.

Because neither Carlson nor Jensenworth, taken alone or in combination, teaches or suggests every element of the Applicants' independent claims 21, 23, and 25, the claims are patentable over Carlson and Jensenworth and should be allowed to issue. Accordingly, the rejection of these claims should be withdrawn. Claim 22 which

depends on claim 21 and claim 24, which depends upon claim 23 should also be allowed to issue as depending upon allowable independent claims (i.e., for at least the reasons presented). Reconsideration of the rejection is respectfully requested.

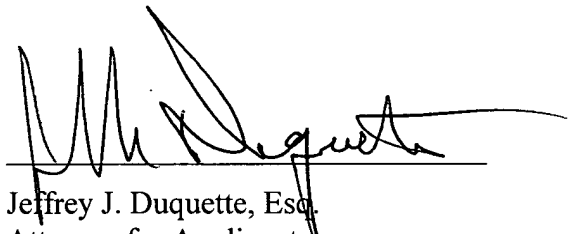
Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after this Amendment, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicant's Representative at the number below.

Applicant hereby petitions for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Amendment, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-0901.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 366-9600, in Westborough, Massachusetts.

Respectfully submitted,



Jeffrey J. Duquette, Esq.
Attorney for Applicants
Registration No.: 45,487
CHAPIN & HUANG, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 366-9600
Facsimile: (508) 616-9805

Attorney Docket No.: EMC00-28(00163)

Dated: October 4, 2004